Have you ever asked yourself the following question: How is my data protected? And for how long? Hello, my name is Asya and I'm happy to present this topic which has captivated me. My problematic will revolve around cyber security in the quantum world; more specifically: how the invention of quantum computers could be a threat to our security. I will first present the security system in place today; I will then tell you the problem that these systems will face in the near future. To conclude, I will put in perspective our current advances and our solutions.

Cyber security is the protection of our data and therefore, in a way, that of our identities. Our security systems today are based on a process called RSA; it is an asymmetric encryption algorithm that allows us to encode and decode messages based on calculations. Unlike the symmetric system, which uses 1 same key to encrypt and decrypt a message, this one uses 2 keys per user. The first one being a public key to which everyone has access, and the second being a private key that only its user can see. Note that it is impossible to calculate the private key from the public key. To illustrate an example: visualize 2 people, by convention, Alice and Bob, who want to send each other private messages (I have made a diagram of the process on the support). In order to do so, Alice will encode her message using Bob's public key. Everybody can see the encoded message, but only Bob can decode it using his private key.

Trying to decode this message by brute force, i.e., trying all possible combinations, would be useless because a 256-bit public key could represent an integer of about 77 digits. RSA is very efficient because in order to break it, it requires calculations of factoring very large prime numbers and we don't have, at the moment, computers powerful enough to make these calculations quickly. With an integer of this order (77 digits), this deciphering would take about 300 000 million years using supercomputers.

However, in the 80's, Richard Feynman stated the first theories of a new technology: the so-called quantum computers; This last one uses quantum calculators with some characteristics of quantum physics of which the superposition and the quantum entanglement. A quantum computer uses a superposition of 0 and 1, it uses qubits and no longer bits, this means that they can represent a combination of 0 and 1 at the same time. The action of intricating them is to make possible all the configurations of the states of the qubits, thus increasing the performance of the computer. I have made a diagram of an example of entanglement with 3 qubits on your support: 3 qubits have 8 possible combinations; before entanglement, we have 3 gauges, and after, we have 8. These are 8 possible quantum states.

Classical computers use electrical signals thanks to electrons. The quantum ones would use photons and not electrons. Unfortunately for cryptography, this represents a danger for our RSA system. Peter Shor, in 1994, figures out an algorithm allowing to break this last one: Shor's algorithm. RSA relies all its security on the fact of finding the divisors of a number n which is a difficult problem with an astronomical calculation time. According to Shor, the calculations of his algorithm are not quantum, but classical; however, the time necessary to these calculations is the problem that quantum computers would solve.

Finally, we see that this RSA system could soon be outdated, thus representing a risk for us and many of our systems. It is therefore necessary to find another way to secure our data before developing this new computer. (If the transition from classical to quantum is badly done, it will be a concern for us. How so? The computing speed of these computers will be too fast and break our security systems before we have the time to react).